Phishing Email Analysis Report – Task 2

1. Overview

This report provides a complete phishing analysis of the file **'sample-1035.eml'**. The goal is to identify indicators of phishing, spoofing behavior, social engineering, and malicious links.

2. Email Header Analysis

- Sender spoofing detected: **no-reply@access-accsecurity.com pretending to be Microsoft**.
- Return-Path mismatch: **bounce@iustozncau.co.uk.**
- Reply-To leads to attacker: **solutionteamrecognizd03@gmail.com.**
- Authentication failed: **SPF=none, DKIM=none, DMARC=permerror.**
- Suspicious IP: **89.144.9.91**

3. Email Body Analysis

- Tracking pixel: **http://thebandalisty.com/track/...**
- Fake security action links: mailto links to attacker Gmail.
- Urgent and fear-based wording: 'Unusual sign.in activity'.
- Poor grammar and formatting inconsistencies.

4. Indicators of Compromise (IOCs)

Emails:
- **no-reply@access-accsecurity.com**
- **bounce@iustozncau.co.uk**
- **solutionteamrecognizd03@gmail.com**

Domains:
- **access-accsecurity.com**
- **iustozncau.co.uk**
- **thebandalisty.com**

IP:
- **89.144.9.91**

URLs:
- **http://thebandalisty.com/track/...**

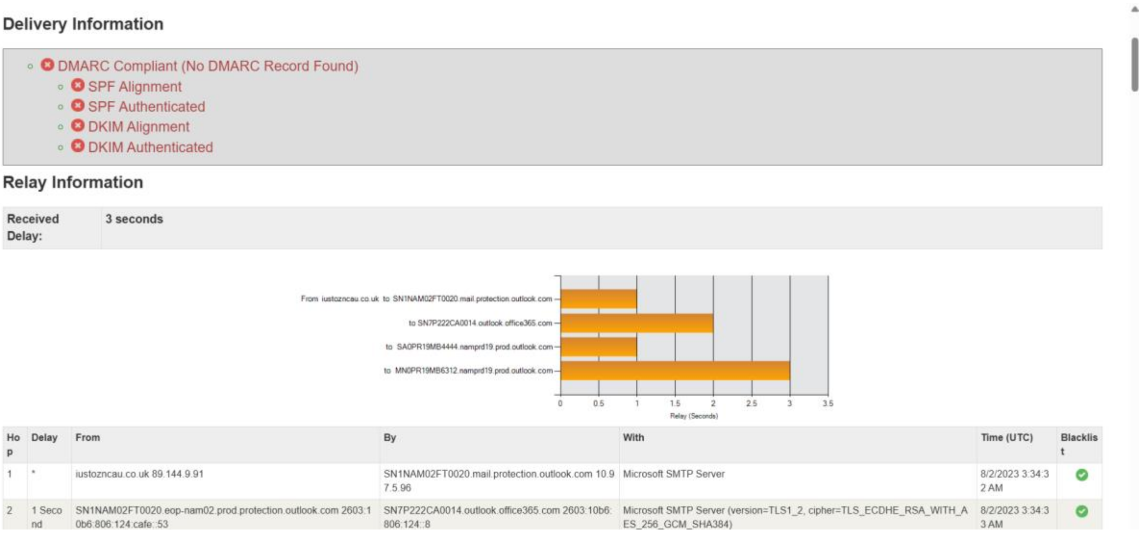
5. Verdict

This is a high-confidence phishing email based on spoofing, failed authentication, suspicious domains, tracking pixel, and social■engineering methods.

6. Recommended Actions

- Do not click or reply.
- Block sender domains and IP.
- Report through security workflow.
- If interacted: reset credentials and check login activity.

SCREENSHOTS OF THE MXTOOLBOX



Delivery Information

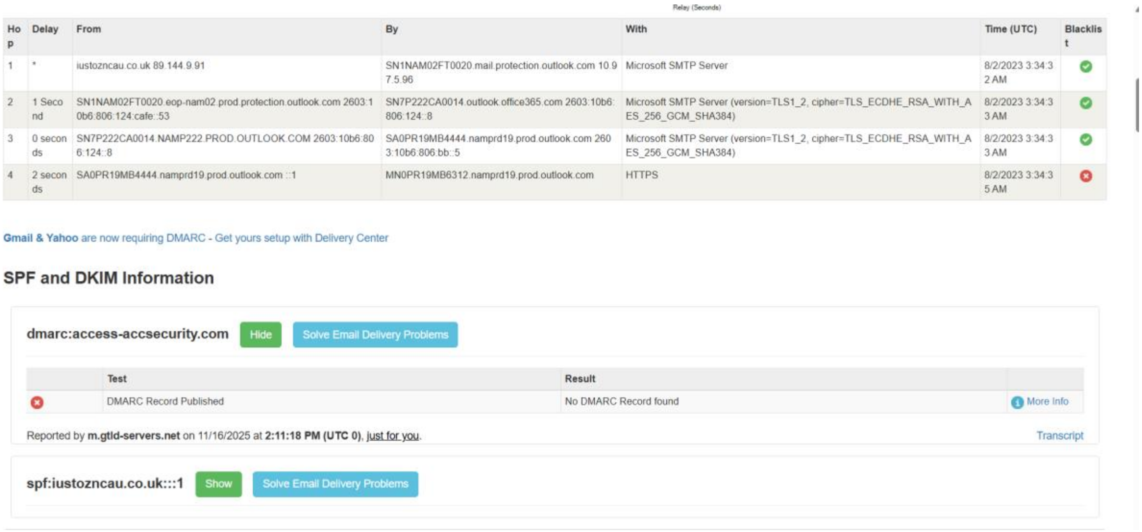
- ✗ DMARC Compliant (No DMARC Record Found)
  - ✗ SPF Alignment
  - ✗ SPF Authenticated
  - ✗ DKIM Alignment
  - ✗ DKIM Authenticated

Relay Information

Received Delay:	3 seconds

From iustozncau.co.uk to SN1NAM02FT0020.mail.protection.outlook.com
to SN7P222CA0014.outlook.office365.com
to SA0PR19MB4444.namprd19.prod.outlook.com
to MN0PR19MB6312.namprd19.prod.outlook.com
0
0.5
1
1.5
2
2.5
3
3.5
Relay (Seconds)

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	iustozncau.co.uk 89.144.9.91	SN1NAM02FT0020.mail.protection.outlook.com 10.97.5.96	Microsoft SMTP Server	8/2/2023 3:34:32 AM	✓
2	1 Second	SN1NAM02FT0020.eop-nam02.prod.protection.outlook.com 2603:10b6:806:124:cafe::53	SN7P222CA0014.outlook.office365.com 2603:10b6:806:124::8	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	8/2/2023 3:34:33 AM	✓



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	iustozncau.co.uk 89.144.9.91	SN1NAM02FT0020.mail.protection.outlook.com 10.97.5.96	Microsoft SMTP Server	8/2/2023 3:34:32 AM	✓
2	1 Second	SN1NAM02FT0020.eop-nam02.prod.protection.outlook.com 2603:10b6:806:124:cafe::53	SN7P222CA0014.outlook.office365.com 2603:10b6:806:124::8	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	8/2/2023 3:34:33 AM	✓
3	0 seconds	SN7P222CA0014.NAMP222.PROD.OUTLOOK.COM 2603:10b6:806:124::8	SA0PR19MB4444.namprd19.prod.outlook.com 2603:10b6:806:bb::5	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	8/2/2023 3:34:33 AM	✓
4	2 seconds	SA0PR19MB4444.namprd19.prod.outlook.com ::1	MN0PR19MB6312.namprd19.prod.outlook.com	HTTPS	8/2/2023 3:34:35 AM	✗

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

SPF and DKIM Information

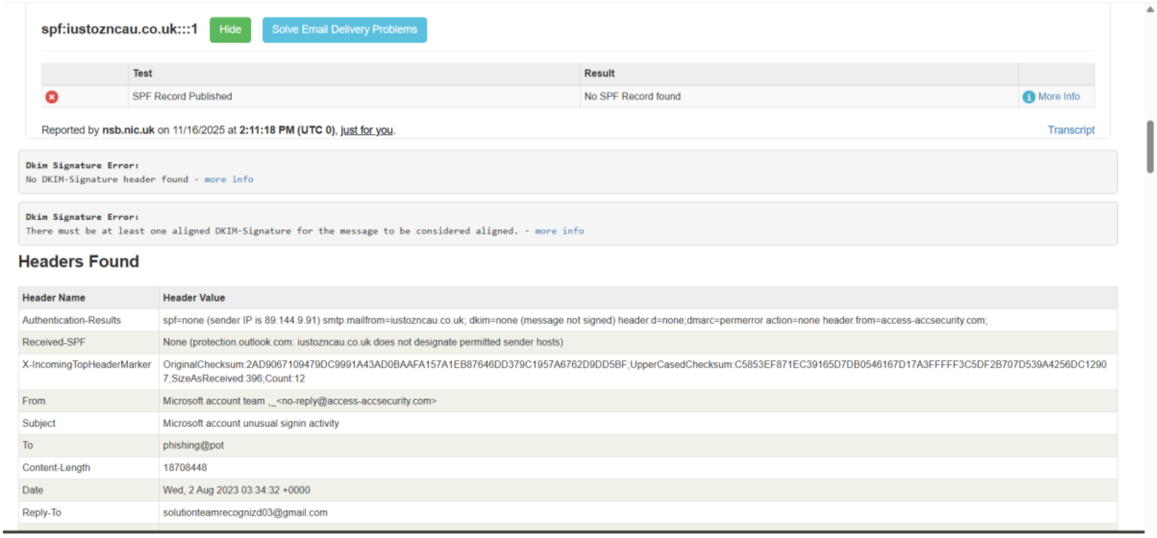
dmarc:access-accsecurity.com

	Test	Result	
✗	DMARC Record Published	No DMARC Record found	More Info

Reported by **m.gtld-servers.net** on 11/16/2025 at **2:11:18 PM (UTC 0)**, just for you.

Transcript

spf:iustozncau.co.uk:::1



spf:iustozncau.co.uk:::1 Hide Solve Email Delivery Problems

	Test	Result	
⊗	SPF Record Published	No SPF Record found	ⓘ More Info

Reported by **nsb.nic.uk** on 11/16/2025 at **2:11:18 PM (UTC 0)**, just for you.

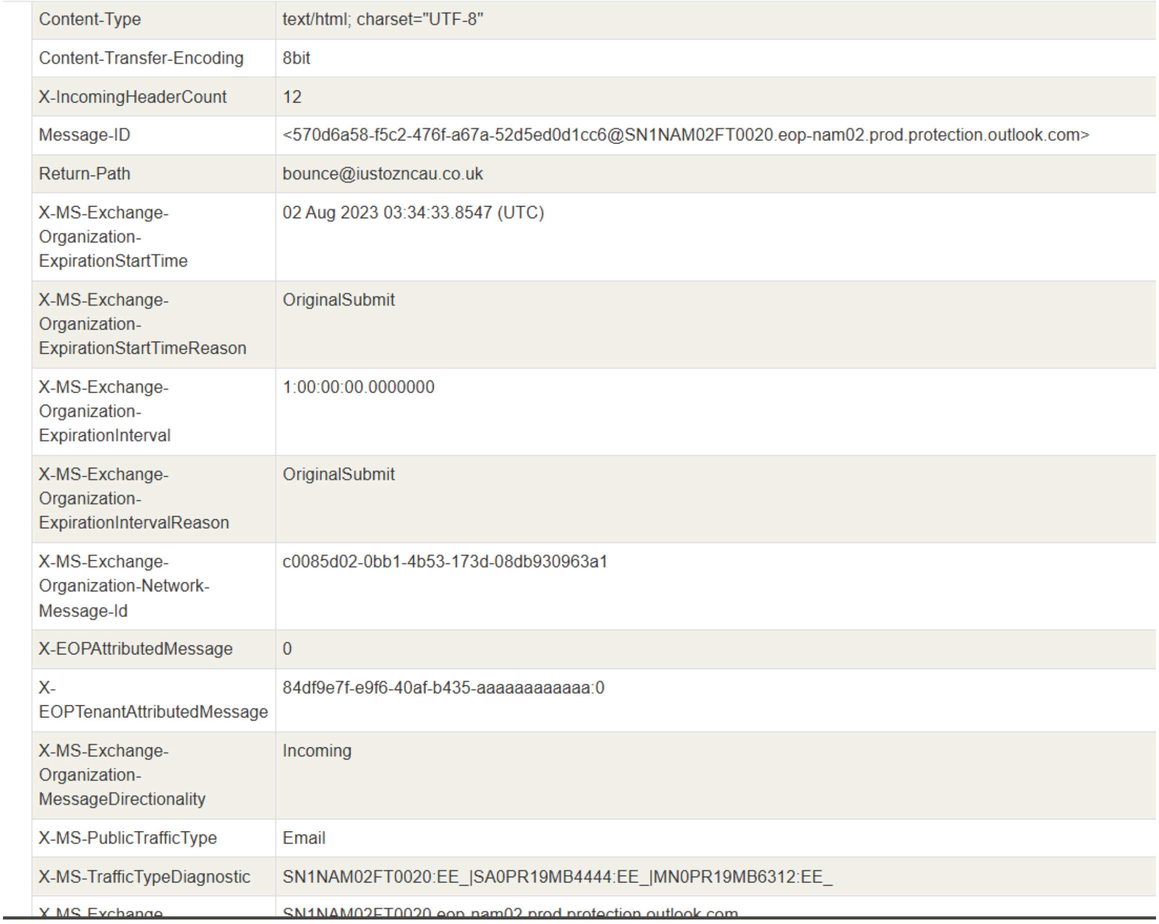
Transcript

```
Dkim Signature Error:
No DKIM-Signature header found - more info
```

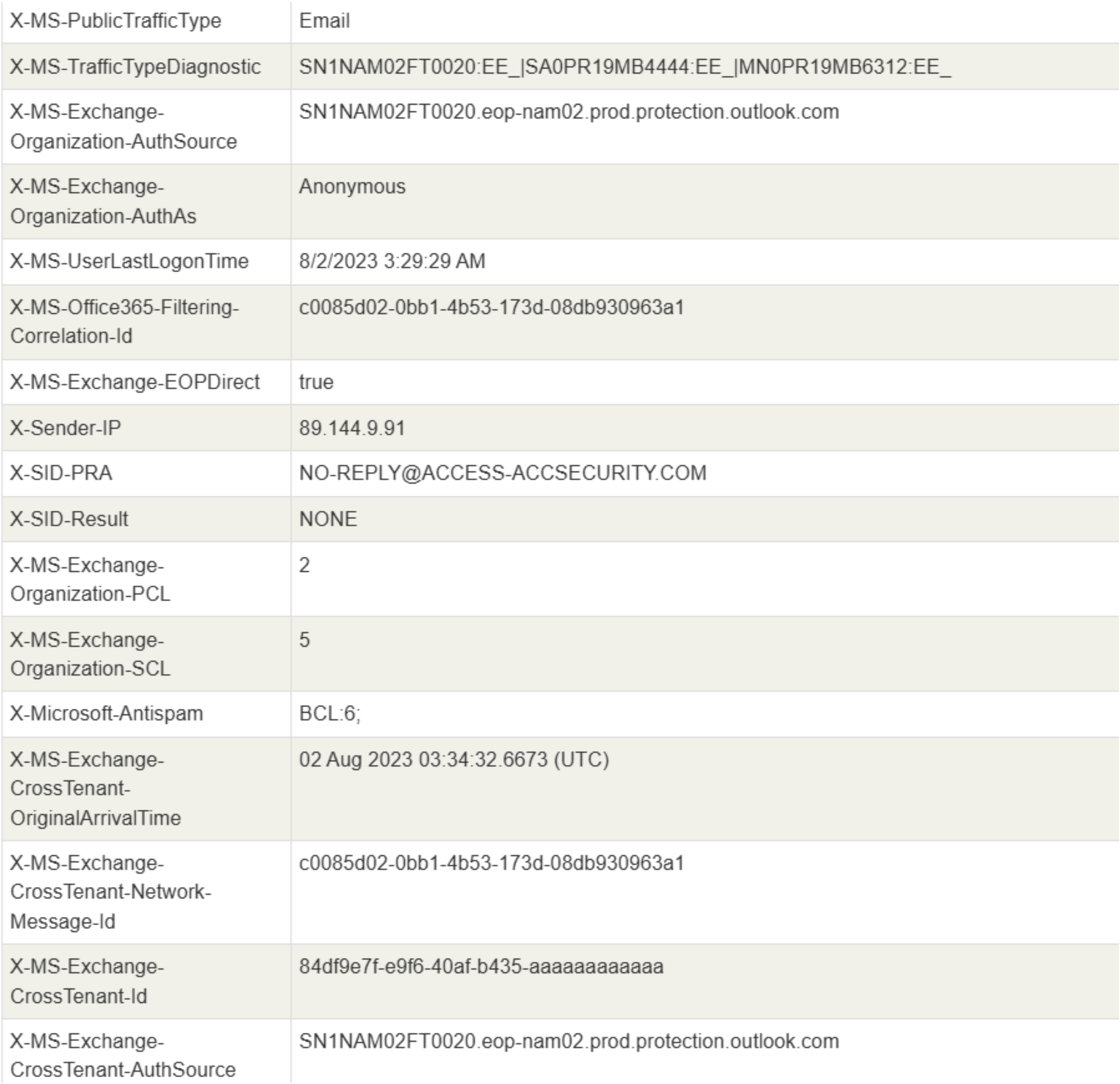
```
Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info
```

Headers Found

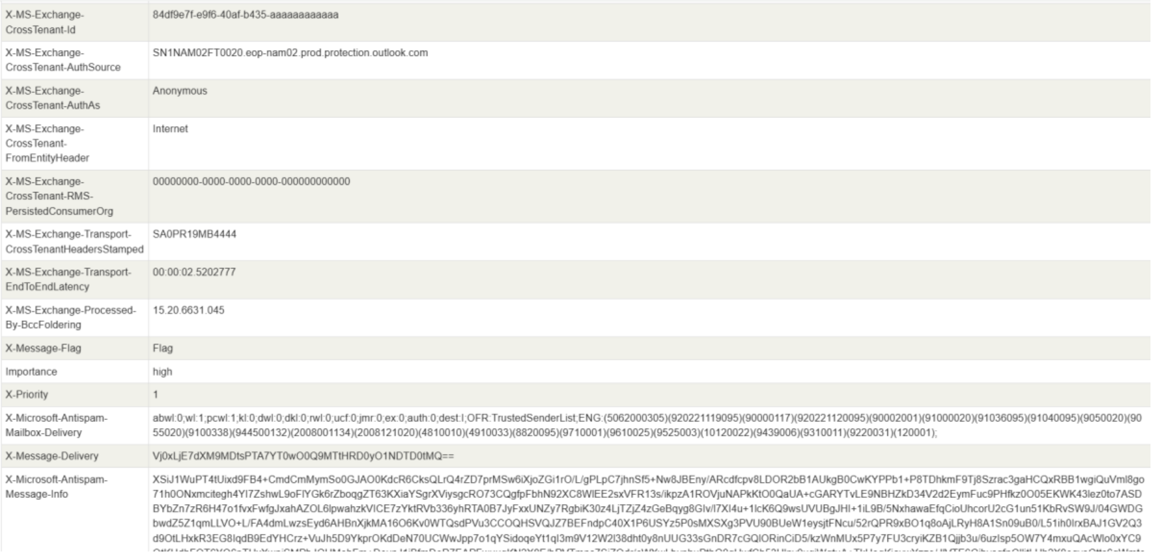
Header Name	Header Value
Authentication-Results	spf=none (sender IP is 89.144.9.91) smtp.mailfrom=iustozncau.co.uk; dkim=none (message not signed) header.d=none;dmarc=permerror action=none header.from=access-accsecurity.com;
Received-SPF	None (protection.outlook.com: iustozncau.co.uk does not designate permitted sender hosts)
X-IncomingTopHeaderMarker	OriginalChecksum:2AD9067109479DC9991A43AD0BAAFA157A1EB87646DD379C1957A6762D9DD5BF;UpperCasedChecksum:C5853EF871EC39165D7DB0546167D17A3FFFFF3C5DF2B707D539A4256DC12907;SizeAsReceived:396;Count:12
From	Microsoft account team ,_<no-reply@access-accsecurity.com>
Subject	Microsoft account unusual signin activity
To	phishing@pot
Content-Length	18708448
Date	Wed, 2 Aug 2023 03:34:32 +0000
Reply-To	solutionteamrecognizd03@gmail.com



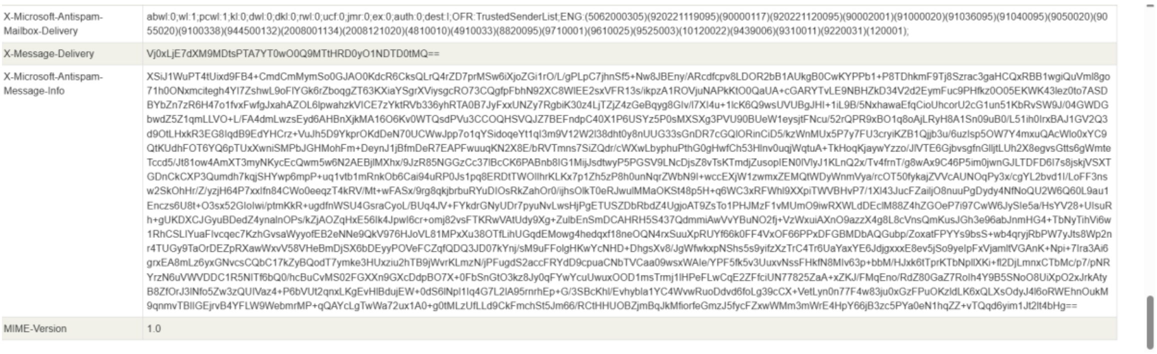
Content-Type	text/html; charset="UTF-8"
Content-Transfer-Encoding	8bit
X-IncomingHeaderCount	12
Message-ID	<570d6a58-f5c2-476f-a67a-52d5ed0d1cc6@SN1NAM02FT0020.eop-nam02.prod.protection.outlook.com>
Return-Path	bounce@iustozncau.co.uk
X-MS-Exchange-Organization-ExpirationStartTime	02 Aug 2023 03:34:33.8547 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason	OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval	1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason	OriginalSubmit
X-MS-Exchange-Organization-Network-Message-Id	c0085d02-0bb1-4b53-173d-08db930963a1
X-EOPAttributedMessage	0
X-EOPTenantAttributedMessage	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
X-MS-Exchange-Organization-MessageDirectionality	Incoming
X-MS-PublicTrafficType	Email
X-MS-TrafficTypeDiagnostic	SN1NAM02FT0020:EE_|SA0PR19MB4444:EE_|MN0PR19MB6312:EE_
X-MS-Exchange	SN1NAM02FT0020.eop-nam02.prod.protection.outlook.com



X-MS-PublicTrafficType	Email
X-MS-TrafficTypeDiagnostic	SN1NAM02FT0020:EE_|SA0PR19MB4444:EE_|MN0PR19MB6312:EE_
X-MS-Exchange-Organization-AuthSource	SN1NAM02FT0020.eop-nam02.prod.protection.outlook.com
X-MS-Exchange-Organization-AuthAs	Anonymous
X-MS-UserLastLogonTime	8/2/2023 3:29:29 AM
X-MS-Office365-Filtering-Correlation-Id	c0085d02-0bb1-4b53-173d-08db930963a1
X-MS-Exchange-EOPDirect	true
X-Sender-IP	89.144.9.91
X-SID-PRA	NO-REPLY@ACCESS-ACCSECURITY.COM
X-SID-Result	NONE
X-MS-Exchange-Organization-PCL	2
X-MS-Exchange-Organization-SCL	5
X-Microsoft-Antispam	BCL:6;
X-MS-Exchange-CrossTenant-OriginalArrivalTime	02 Aug 2023 03:34:32.6673 (UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id	c0085d02-0bb1-4b53-173d-08db930963a1
X-MS-Exchange-CrossTenant-Id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
X-MS-Exchange-CrossTenant-AuthSource	SN1NAM02FT0020.eop-nam02.prod.protection.outlook.com

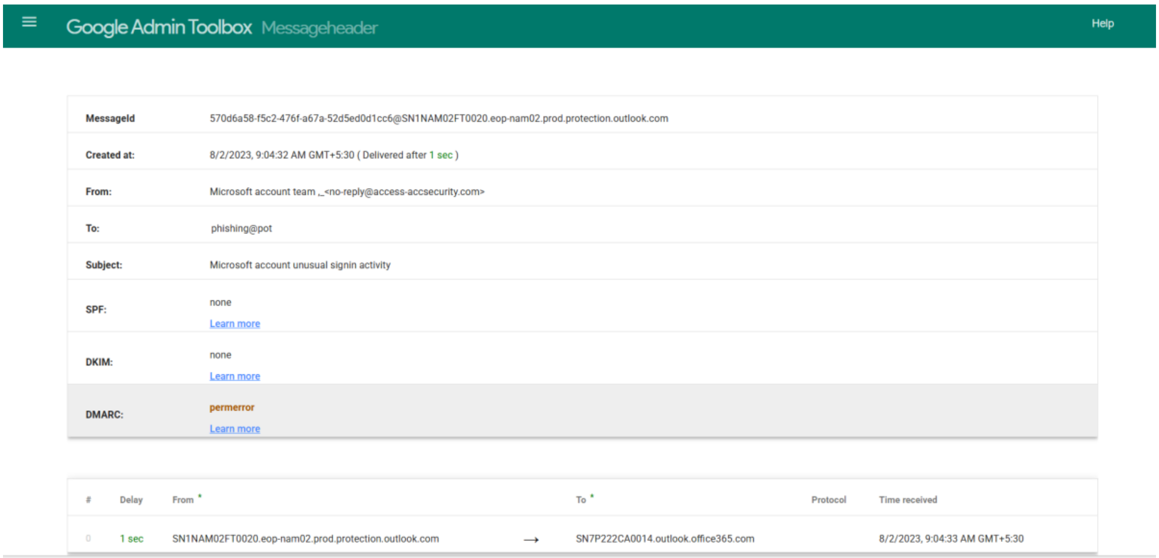


X-MS-Exchange-CrossTenant-Id	84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
X-MS-Exchange-CrossTenant-AuthSource	SN1NAM02FT0020.eop-nam02.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-AuthAs	Anonymous
X-MS-Exchange-CrossTenant-FromEntityHeader	Internet
X-MS-Exchange-CrossTenant-RMS-PersistedConsumerOrg	00000000-0000-0000-0000-000000000000
X-MS-Exchange-Transport-CrossTenantHeadersStamped	SA0PR19MB4444
X-MS-Exchange-Transport-EndToEndLatency	00:00:02.5202777
X-MS-Exchange-Processed-By-BccFoldering	15.20.6631.045
X-Message-Flag	Flag
Importance	high
X-Priority	1
X-Microsoft-Antispam-Mailbox-Delivery	abwl:0;wl:1;pcwl:1;kl:0;dwl:0;dkl:0;rwl:0;ucf:0;jmr:0;ex:0;auth:0;dest:I;OFR:TrustedSenderList;ENG:(5062000305)(920221119095)(90000117)(920221120095)(90002001)(91000020)(91036095)(91040095)(9050020)(9055020)(9100338)(944500132)(2008001134)(2008121020)(4810010)(4910033)(8820095)(9710001)(9610025)(9525003)(10120022)(9439006)(9310011)(9220031)(120001);
X-Message-Delivery	Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MTtHRD0yO1NDTD0tMQ==
X-Microsoft-Antispam-Message-Info	XSiJ1WuPT4tUixd9FB4+CmdCmMymSo0GJAO0KdcR6CksQLrQ4rZD7prMSw6iXjoZGi1rO/L/gPLpC7jhnSf5+Nw8JBEny/ARcdfcpv8LDOR2bB1AUkgB0CwKYPPb1+P8TDhkmF9Tj8Szrac3gaHCQxRBB1wgiQuVml8go71h0ONxmcitegh4Yl7ZshwL9oFlYGk6rZboqgZT63KXiaYSgrXViysgcRO73CQgfpFbhN92XC8WlEE2sxVFR13s/ikpzA1ROVjuNAPkKtO0QaUA+cGARYTvLE9NBHZkD34V2d2EymFuc9PHfkz0O05EKWK43lez0to7ASDBYbZn7zR6H47o1fvxFwfgJxahAZOL6lpwahzkVICE7zYktRVb336yhRTA0B7JyFxxUNZy7RgbiK30z4LjTZjZ4zGeBqyg8Glv/l7Xl4u+1lcK6Q9wsUVUBgJHl+1iL9B/5NxhawaEfqCioUhcorU2cG1un51KbRvSW9J/04GWDGbwdZ5Z1qmLLVO+L/FA4dmLwzsEyd6AHBnXjkMA16O6Kv0WTQsdPVu3CCOQHSVQJZ7BEFndpC40X1P6USYz5P0sMXSXg3PVU90BUeW1eysjtFNcu/52rQPR9xBO1q8oAjLRyH8A1Sn09uB0/L51ih0lrxBAJ1GV2Q3d9OtLHxkR3EG8lqdB9EdYHCrz+VuJh5D9YkprOKdDeN70UCWwJpp7o1qYSidoqeYt1ql3m9V12W2l38dht0y8nUUG33sGnDR7cGQlORinCiD5/kzWnMUx5P7y7FU3cryiKZB1Qjjb3u/6uzIsp5OW7Y4mxuQAcWlo0xYC9



X-Microsoft-Antispam-Mailbox-Delivery	abwl:0;wl:1;pcwl:1;kl:0;dwl:0;dkl:0;rwl:0;ucf:0;jmr:0;ex:0;auth:0;dest:I;OFR:TrustedSenderList;ENG:(5062000305)(920221119095)(90000117)(920221120095)(90002001)(91000020)(91036095)(91040095)(9050020)(9055020)(9100338)(944500132)(2008001134)(2008121020)(4810010)(4910033)(8820095)(9710001)(9610025)(9525003)(10120022)(9439006)(9310011)(9220031)(120001);
X-Message-Delivery	Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MTtHRD0yO1NDTD0tMQ==
X-Microsoft-Antispam-Message-Info	XSiJ1WuPT4tUixd9FB4+CmdCmMymSo0GJAO0KdcR6CksQLrQ4rZD7prMSw6iXjoZGi1rO/L/gPLpC7jhnSf5+Nw8JBEny/ARcdfcpv8LDOR2bB1AUkgB0CwKYPPb1+P8TDhkmF9Tj8Szrac3gaHCQxRBB1wgiQuVml8go71h0ONxmcitegh4YI7ZshwL9oFlYGk6rZboqgZT63KXiaYSgrXViysgcRO73CQgfpFbhN92XC8WIEE2sxVFR13s/ikpzA1ROVjuNAPkKtO0QaUA+cGARYTvLE9NBHZkD34V2d2EymFuc9PHfkz0O05EKWK43lez0to7ASDBYbZn7zR6H47o1fvxFwfgJxahAZOL6lpwahzkVICE7zYktRVb336yhRTA0B7JyFxxUNZy7RgbiK30z4LjTZjZ4zGeBqyg8GIv/I7XI4u+1lcK6Q9wsUVUBgJHI+1iL9B/5NxhawaEfqCioUhcorU2cG1un51KbRvSW9J/04GWDGbwdZ5Z1qmLLVO+L/FA4dmLwzsEyd6AHBnXjkMA16O6Kv0WTQsdPVu3CCOQHSVQJZ7BEFndpC40X1P6USYz5P0sMXSXg3PVU90BUeW1eysjtFNcu/52rQPR9xBO1q8oAjLRyH8A1Sn09uB0/L51ih0IrxBAJ1GV2Q3d9OtLHxkR3EG8IqdB9EdYHCrz+VuJh5D9YkprOKdDeN70UCWwJpp7o1qYSidoqeYt1qI3m9V12W2I38dht0y8nUUG33sGnDR7cGQIORinCiD5/kzWnMUx5P7y7FU3cryiKZB1Qjjb3u/6uzIsp5OW7Y4mxuQAcWlo0xYC9QtKUdhFOT6YQ6pTUxXwniSMPbJGHMohFm+DeynJ1jBfmDeR7EAPFwuuqKN2X8E/bRVTmns7SiZQdr/cWXwLbyphuPthG0gHwfCh53HInv0uqjWqtuA+TkHoqKjaywYzzo/JIVTE6GjbvsgfnGlljtLUh2X8egvsGtts6gWmteTccd5/Jt81ow4AmXT3myNKycEcQwm5w6N2AEBjlMXhx/9JzR85NGGzCc37lBcCK6PABnb8IG1MijJsdtwyP5PGSV9LNcDjsZ8vTsKTmdjZusopIEN0lVlyJ1KLnQ2x/Tv4frnT/g8wAx9C46P5im0jwnGJLTDFD6I7s8jskjVSXTGDnCkCXP3Qumdh7kqjSHYwp6mpP+uq1vtb1mRnkOb6Cai94uRP0Js1pq8ERDtTWOIlhrKLKx7p1Zh5zP8h0unNqrZWbN9I+wccEXjW1zwmxZEMQtWDyWnmVya/rcOT50fykajZVVcAUNOqPy3x/cgYL2bvd1I/LoFF3nsw2SkOhHr/Z/yzjH64P7xxIfn84CWo0eeqzT4kRV/Mt+wFASx/9rg8qkjbrbuRYuDIOsRkZahOr0/ijhsOlkT0eRJwulMMaOKSt48p5H+q6WC3xRFWhl9XXpiTWVBHvP7/1XI43JucFZailjO8nuuPgDydy4NfNoQU2W6Q60L9au1Enczs6U8t+O3sx52GIolwi/ptmKkR+ugdfnWSU4GsraCyoL/BUq4JV+FYkdrGNyUDr7pyuNvLwsHjPgETUSZDbRbdZ4UgjoAT9ZsTo1PHJMzF1vMUmO9iwRXWLdDEclM88Z4hZGOeP7i97CwW6JySle5a/HsYV28+UIsuRh+gUKDXCJGyuBDedZ4ynalnOPs/kZjAOZqHxE56lk4Jpwl6cr+omj82vsFTKRwVAtUdy9Xg+ZulbEnSmDCAHRH5S437QdmmiAwVvYBuNO2fj+VzWxuiAXnO9azzX4g8L8cVnsQmKusJGh3e96abJnmHG4+TbNyTihVi6w1RhCSLIYuaFlvcqec7KzhGvsaWyyofEB2eNNe9QkV976HJoVL81MPxXu38OTfLihUGqdEMowg4hedqxf18neOQN4rxSuuXpRUYf66k0FF4VxOF66PPxDFGBMDbAQGubp/ZoxatFPYYs9bsS+wb4qryjRbPW7yJts8Wp2nr4TUGy9TaOrDEZpRXawWxvV58VHeBmDjSX6bDEyyPOVeFCZqfQDQ3JD07kYnj/sM9uFFolgHKwYcNHD+DhgsXv8/JgWfwkxpNShs5s9yifzXzTrC4Tr6UaYaxYE6JdjgxxxE8ev5jSo9yelpFxVjamltVGAnK+Npi+7lra3Ai6grxEA8mLz6yxGNvcsCQbC17kZyBQodT7ymke3HUxziu2hTB9jWvrKLmzN/jPFugdS2accFRYdD9cpuaCNbTVCaa09wsxWAle/YPF5fk5v3UuxvNssFHkfN8MIv63p+bbM/HJxk6tTprKTbNpllXKi+fl2DjLmnxCTbMc/p7/pNRYrzN6uVWVDDC1R5NITf6bQ0/hcBuCvMS02FGXXn9GXcDdpBO7X+0FbSnGtO3kz8Jy0qFYwYcuUwuxOOD1msTrmj1lHPeFLwCqE2ZFfciUN77825ZaA+xZKJ/FMqEno/RdZ80GaZ7Rolh4Y9B5SNoO8UiXpO2xJrkAtyB8ZfOrJ3lNfo5Zw3zQUIVaz4+P6bVUt2qnxLKgEvHlBdujEW+0dS6lNpl1Iq4G7L2lA95rnrhEp+G/3SBcKhl/Evhybla1YC4WvwRuoDdvd6foLg39cCX+VetLyn0n77F4w83ju0xGzFPuOKzldLK6xQLXsOdyJ4l6oRWEhnOukM9qnmvTBIlGEjrvB4YFLW9WebmrMP+qQAYcLgTwWa72ux1A0+g0tMLzUfLLd9CkFmchSt5Jm66/RCtHHUOBZjmBqJkMfiorfeGmzJ5fycFZxwWMm3mWrE4HpY66jB3zc5PYa0eN1hqZZ+vTQqd6yim1Jt2lt4bHg==
MIME-Version	1.0

GOOGLE ADMIN TOOLBOX SCREENSHOTS



MessageId	570d6a58-f5c2-476f-a67a-52d5ed0d1cc6@SN1NAM02FT0020.eop-nam02.prod.protection.outlook.com
Created at:	8/2/2023, 9:04:32 AM GMT+5:30 (Delivered after 1 sec)
From:	Microsoft account team ,_<no-reply@access-accsecurity.com>
To:	phishing@pot
Subject:	Microsoft account unusual signin activity
SPF:	none Learn more
DKIM:	none Learn more
DMARC:	permerror Learn more

#	Delay	From *		To *	Protocol	Time received
0	1 sec	SN1NAM02FT0020.eop-nam02.prod.protection.outlook.com	→	SN7P222CA0014.outlook.office365.com		8/2/2023, 9:04:33 AM GMT+5:30